UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/696,200	10/28/2003	David M. Chess	GB920030050US1	7325

66517 7590 06/06/2012

STEVEN E. BACH, ATTORNEY AT LAW
10 ROBERTS ROAD
NEWTOWN SQUARE, PA 19073

EXAMINER	
HOANG, DANIEL L	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
06/06/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DAVID M. CHESS
and JAMES S. LUKE

Appeal 2010-003743
Application 10/696,200
Technology Center 2400

Before KALYAN K. DESHPANDE, MICHAEL R. ZECHER, and JOHNNY A. KUMAR, *Administrative Patent Judges*.

KUMAR, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1-15. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Appellants' Invention

Appellants' invention relates to detecting malicious software within or attacking a computer system. *See* Abstract.

Illustrative Claim

1. A method for detecting malicious software within or attacking a computer system, said method comprising the steps of:

In response to a system call, executing a hook routine at a location of said system call to (a) determine a data flow or process requested by said call, (b) determine another data flow or process for data related to that of said call, (c) automatically generate a consolidated information flow diagram showing said data flow or process of said call and said other data flow or process, and after steps (a-c), (d) call a routine to perform said data flow or process requested by said call.

Prior Art Relied Upon

Hollander	US 6,823,460 B1	Nov. 23, 2004

Rejection on Appeal

Claims 1-15 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Hollander.[1] Ans. 3-5.

[1] We note the Examiner's typographical error of rejecting the claims under "35 USC 102(b)", rather than "35 USC 102(e)". We also note that the Examiner has quoted the text of 35 U.S.C. § 102(e). Ans. 3. For the purpose of this opinion, we will treat Hollander as a 35 U.S.C. § 102(e) reference. Moreover, while the Examiner only includes claims 1-14 in the statement of the rejection (Ans. 3), the Examiner nonetheless includes claim 15 in the

ISSUES

The Examiner finds that Hollander anticipates claims 1-15. Ans. 3-5. Appellants argue that Hollander does not teach all the claimed features. Br. 8-17.[2]

Has the Examiner erred in rejecting representative independent claim 1 by finding that Hollander discloses the claim limitations: (1) "[i]n response to a system call, executing a hook routine at a location of said system call"; (2) "determine a dataflow or process requested by said call"; (3) "determine another data flow or process for data related to that of said call"; and (4) "automatically generate a consolidated information flow diagram showing said data flow or process of said call and said other data flow or process"?

ANALYSIS

Claims 1, 8 and 14[3]

At the outset, we have reviewed the Examiner's rejections in light of Appellants' contentions that the Examiner has erred. We disagree with

---

body of the rejection. *Id.* at 5. We will treat the Examiner's incorrect statement of the rejection as mere harmless error and, therefore, presume that the Examiner intended to reject claim 15 under 35 U.S.C. § 102(e) as being anticipated by Hollander. *Accord* Br. 7, (confirming that claim 15 is rejected under 35 U.S.C. § 102(e)).

[2] All references to the Brief refer to the Brief filed July 8, 2009, which replaced the Brief filed on March 23, 2009.

[3] Appellants offer the same arguments set forth in response to the anticipation rejection of independent claim 1 to rebut the anticipation rejection of independent claims 8 and 14. *See* Br. 8-14

Appellants' conclusions. We agree with and adopt as our own (1) the findings and reasons set forth by the Examiner in the action from which this appeal is taken and (2) the reasons set forth by the Examiner in the Answer in response to Appellants' Appeal Brief.

In particular, Appellants first contend that Hollander does not disclose executing a hook routine in response to a system call. Br. 9. We begin our analysis by first considering the scope and meaning of the claim term "hook," which must be given its broadest reasonable interpretation consistent with Appellants' disclosure. *See In re Morris*, 127 F.3d 1048, 1054 (Fed. Cir. 1997); *see also In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989) (stating that during examination "claims must be interpreted as broadly as their terms reasonably allow").

The Appellants describe hooking in their Specification (page 7, ll. 27-28) as "the insertion of an additional routine at a call location in an operating system or other program and relocating the original, called routine from the call location." The Appellants admit that Hollander discloses overwriting a section or sections of the application program interface routines ("API") to control the code behavior (Br. 10). The Examiner equates Hollander's injecting of an API Interception Module (fig, 2, element 56) into all active processes to the claimed hook routine. *See* Ans. 6 (citing Hollander at Fig. 2 (step 56). Since the Examiner's position is consistent with our claim construction *supra*, we agree with the Examiner's findings.

The Appellants next contend that Hollander does not disclose determining a data flow or process (or another data flow or process) as requested by the system call. Br. 11-12. Specifically, Appellants contend

that Hollander does not disclose or suggest stringing together related system call operations to track data flow or process flows. *Id.*

The Examiner finds that Hollander discloses process creation (step 60) that corresponds to the claimed data process and process termination (step 62) that corresponds to the another data process. *See* Ans. 6 (citing to col. 6, lines 7-20 of Hollander). We agree with the Examiner.

Finally, Appellants contend that Hollander does not disclose generating a consolidated information flow diagram. Br. 13. In particular, Appellants contend that Hollander's API flow table is not analogous to the consolidated information flow diagram as recited in claim 1. Br. 13. We disagree with the Appellants.

The Examiner finds that Hollander discloses the steps of saving the address of API functions to an API Flow structure table that correspond to the claimed information flow diagram. Ans. 7 (citing to Hollander fig. 7, elements 154, 156, 160, 162). We agree with the Examiner.

With regard to Appellants' contention that Hollander does not describe the "display screen" recited in claim 8 (Br. 15), we are not persuaded by Appellants' arguments because a display screen necessarily flows from the computer system (col. 13, lines 39-40) disclosed in Hollander.

Thus, we find that Hollander sufficiently describes the disputed claim limitations. It follows that the Examiner has not erred in finding that Hollander anticipates independent claims 1, 8, and 14.

Claim 2

Claim 2 depends from claim 1 and recites *inter alia*: "a user monitors said information flow diagram." We agree with the Examiner's finding that Hollander discloses (col. 11, lines 23-50), manipulating a process-level flow control structure as per user pre-defined or user online instructions in order to decide whether to allow an API function to execute. Ans. 9. Thus, we find that Hollander describes the disputed claim limitation. It follows that the Examiner has not erred in finding that Hollander anticipates dependent claim 2.

Claims 3 and 9

Claims 3 and 9 depend from claims 1 and 8 respectively and recite "said information flow diagram illustrates locations of said data at stages of a processing activity." We agree with the Examiner's finding that Hollander's steps 154-165[4] correspond to the disputed claim limitation. Ans. 9. It follows that the Examiner has not erred in finding that Hollander anticipates dependent claims 3 and 9.

Claims 4-7, 10-13, and 15

Appellants do not provide separate and distinct arguments for patentability with respect to dependent claims 4-7, 10-13, and 15. *See* Br. 8-17. Therefore, these claims fall with their respective independent claims 1, 8, and 14. *See* 37 C.F.R. § 41.37(c)(1)(vii).

[4] We note the clerical error in the Answer of a reference to Fig 3 instead of Fig. 7 in Hollander for steps 154-165. The Examiner has cited the correct reference to Fig. 7 for the "information flow diagram" recited in independent claims 1 and 8. Ans. 3-4.

IV. CONCLUSION

The Examiner has not erred in rejecting claims 1-15 as being anticipated under 35 U.S.C. § 102(e).

V. DECISION

We affirm the Examiner's decision to reject claims 1-15 as being anticipated under 35 U.S.C. § 102(e).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

msc